ESET ENDPOINT SECURITY

FÜR ANDROID

Installations- und Benutzerhandbuch

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen

Inhalt

1. Installation von ESET Endpoint Security 3
1.1 Installation 3
1.2 Deinstallation 4
2. Produktaktivierung 4
3. Antivirus 4
4. USSD-Steuerung 6
5. Antispam 7
6. Anti-Theft 8
7. Sicherheits-Audit 9
8. Remoteverwaltung 10
9. Update 11
10. Passwort 11
11. Fehlerbehebung und Support 12
11.1 Fehlerbehebung 12
11.2 Support 12

ESET **ENDPOINT SECURITY**

Copyright © ©2012 ESET, spol. s r.o.
ESET Endpoint Security wurde entwickelt von ESET, spol. s r.o.
Weitere Informationen finden Sie unter www.eset.com.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung an jedem der hier beschriebenen Software-Produkte Änderungen vorzunehmen.

Support www.eset.com/support

Stand 17. 12. 2012

1. Installation von ESET Endpoint Security

Zur Installation von ESET Endpoint Security unter Android muss Ihr Mobiltelefon mindestens folgende Systemanforderungen erfüllen:

	Mindest-Systemanforderungen
Betriebssystem	Android 2.1 (Eclair) oder höher
CPU	600 MHz
RAM	256 MB
Freier Platz - interner Speicher	5 MB

HINWEIS: Bestimmte Funktionen (z. B. Spam-Schutz und Anti-Theft) sind auf Android 3.0 bzw. auf Tablets, die Telefonie und Messaging nicht unterstützen, nicht verfügbar. Weitere Details finden Sie in diesem Knowledgebase-Artikel (möglicherweise nicht in Ihrer Sprache verfügbar).

1.1 Installation

Wählen Sie eine der folgenden Methode, um ESET Endpoint Security zu installieren:

- Laden Sie die Installationsdatei *(ees.apk)* für ESET Endpoint Security von der ESET-Website herunter, indem Sie den folgenden QR-Code mit einer App wie QR Droid oder Barcode Scanner einscannen:

- Laden Sie die Datei *ees.apk* von der ESET-Website auf Ihren Computer herunter. Kopieren Sie die Datei per Bluetooth oder über den USB-Anschluss auf Ihr Gerät. Tippen Sie auf dem Android-Hauptbildschirm auf das Übersichtssymbol oder auf **Startseite** > **Menü** und dort auf **Einstellungen** > **Anwendungen.** Achten Sie darauf, dass die Option **Unbekannte Herkunft** aktiviert ist. Suchen Sie die Datei *ees.apk* mit einer App wie ASTRO File Manager oder ES File Explorer. Öffnen Sie die Datei und tippen Sie auf **Installieren**. Nachdem die App installiert wurde, tippen Sie auf **Öffnen**.

- Wenn Sie ESET Endpoint Security auf mehreren Geräten installieren und aktivieren möchten, erstellen Sie in ESET Configuration Editor eine XML-Konfigurationsdatei.

  Öffnen Sie ESET Configuration Editor über die ERA Console (**Tools** > ESET Configuration Editor) oder über **Start** > **Alle Programme** > **ESET** > ESET Remote Administrator**-Konsole >** ESET Configuration Editor. Wählen Sie links im Baum **Mobilgeräte** > **Endpoint Security für Android** > **Update** > **Einstellungen** > **Benutzername**. Geben Sie Ihren Benutzernamen (aus den Lizenzdaten, die Sie nach dem Kauf von ESET erhalten haben) rechts im Feld **Wert** ein und klicken Sie auf **Weiter**. Klicken Sie auf **Passwort festlegen** und geben Sie Ihr Passwort ein. Klicken Sie zum Bestätigen auf **OK** . Mit dem ESET Configuration Editor können Sie außerdem zusätzliche Einstellungen festlegen (z. B. zu Remote Administration oder für den Virenschutz), die auf alle Mobilendgeräte angewendet werden sollen. Wenn Sie alle erwünschten Änderungen vorgenommen haben, klicken Sie auf **Datei** > **Speichern** (oder klicken Sie auf Ctrl+S) und speichern Sie die Datei unter *settings.xml*.

  Kopieren Sie die soeben gespeicherte Datei zusammen mit der ESET Endpoint Security-Installationsdatei „*ees.apk*" (hier verfügbar) in das Stammverzeichnis Ihrer SD-Karte *(/mnt/sdcard)*. Suchen Sie die Datei *ees.apk* mit einer App wie ASTRO File Manager oder ES File Explorer, und tippen Sie auf **Installieren**. Tippen Sie nach Abschluss der Installation auf **Öffnen**. ESET Endpoint Security wird automatisch mit dem in der Datei *settings.xml* gespeicherten Benutzernamen und Passwort aktiviert.

Warnung: ESET Endpoint Security muss im internen Gerätespeicher installiert werden. Einige Mobiltelefone lassen eine Installation von Anwendungen auf der SD-Karte zu. Wenn Sie ESET Endpoint Security auf der SD-Karte installieren, funktionieren der Echtzeit-Dateischutz, der Spam-Schutz und die Anti-Theft-Funktion nicht.

Nach erfolgreicher Installation aktivieren Sie ESET Endpoint Security, indem Sie die Schritte im Abschnitt Produktaktivierung 4 ausführen.

1.2 Deinstallation

Um ESET Endpoint Security von Ihrem Gerät zu deinstallieren, starten Sie über das Hauptmenü von ESET Endpoint Security den **Deinstallationsassistenten** oder führen die folgenden Schritte aus:

1. Tippen Sie auf dem Android-Hauptbildschirm auf das Übersichtssymbol (oder auf **Startseite** > **Menü**). Tippen Sie dann auf **Einstellungen** > **Standort & Sicherheit** > **Geräte-Administratoren**, deaktivieren Sie **ESET Security** und tippen Sie auf **Deaktivieren**. Geben Sie bei der Abfrage Ihr Passwort für ESET Endpoint Security ein. (Wenn Sie ESET Endpoint Security nicht als Geräteadministrator eingerichtet haben, überspringen Sie diesen Schritt.)
2. Kehren Sie zurück in den Bereich **Einstellungen**, und tippen Sie auf **Anwendungen** > **Anwendungen verwalten** > **ESET Security** > **Deinstallieren**.

ESET Endpoint Security und der Quarantäneordner werden endgültig von Ihrem Mobilgerät gelöscht.

2. Produktaktivierung

Nach erfolgreicher Installation muss ESET Endpoint Security aktiviert werden. Tippen Sie dazu im Hauptmenü von ESET Endpoint Security auf **Jetzt aktivieren**.

Aktivierung mit Benutzername und Passwort – Geben Sie den Benutzernamen und das Passwort (die Lizenzdaten, die Sie beim Kauf des Produkts von ESET erhalten haben) in den entsprechenden Feldern ein.

Die Aktivierung ist nur für einen begrenzten Zeitraum gültig. Nach Ablauf der Aktivierungsdauer können Sie die Programmlizenz verlängern. Hierzu erhalten Sie vorab einen Hinweis.

HINWEIS: Während der Aktivierung muss das Gerät mit dem Internet verbunden sein. Es wird eine kleine Datenmenge heruntergeladen.

Standardmäßig wird ESET Endpoint Security in der Sprache installiert, die in den Sprach- und Tastatureinstellungen Ihres Telefons als Systemgebietsschema eingerichtet ist. Um die Anzeigesprache der Benutzeroberfläche zu ändern, tippen Sie im Hauptmenü von ESET Endpoint Security auf **Sprache** und wählen Sie die gewünschte Sprache.

3. Antivirus

Gerät scannen

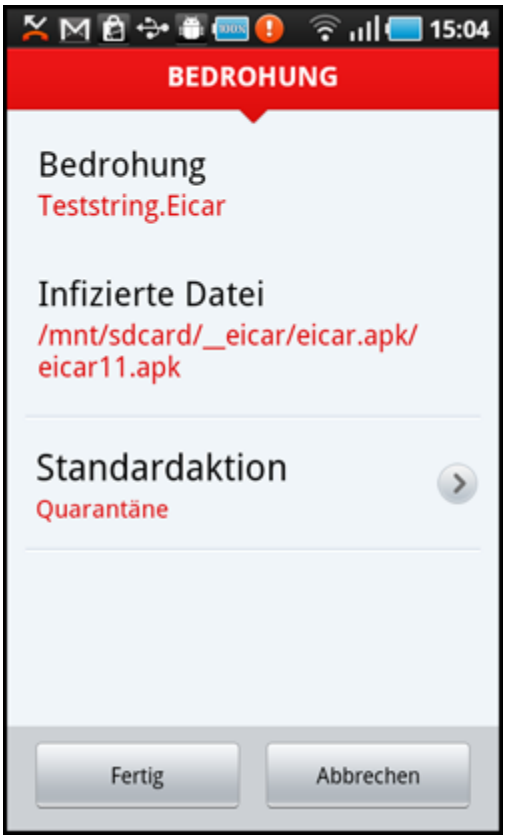
Mit der Option **Gerät scannen** können Sie Ihr Mobilgerät auf Infiltrationen (eingedrungene Schadsoftware) überprüfen.

Bestimmte vordefinierte Dateitypen werden standardmäßig geprüft. Bei einem Scan des gesamten Geräts werden der Arbeitsspeicher, ausgeführte Prozesse, die dazugehörigen Funktionsbibliotheken und Dateien geprüft, die sich im internen Speicher oder auf Wechselmedien befinden. Nach Abschluss des Scans wird eine kurze Zusammenfassung angezeigt (Anzahl der infizierten und gescannten Dateien, Scan-Dauer usw.).

Um einen laufenden Scan abzubrechen, tippen Sie auf **Abbrechen**.

Ordner scannen

Um bestimmte Ordner auf Ihrem Gerät zu scannen, tippen Sie auf **Ordner scannen**. Suchen Sie die gewünschten Ordner, tippen Sie auf die dazugehörigen Kontrollkästchen in der rechten Spalte und dann auf **Scannen**.



Bedrohung erkannt von ESET Endpoint Security

Scan-Logs

Der Bereich **Scan-Logs** enthält Logs mit umfassenden Daten zu abgeschlossenen Scans. Die Logs werden erstellt, wenn ein manuell ausgelöster Scan (On-Demand-Scan) abgeschlossen wurde oder wenn der Echtzeit-Schutz eingedrungene Schadsoftware erkennt.

Jeder Log-Eintrag enthält die folgenden Angaben:

- Datum und Uhrzeit des Ereignisses
- Anzahl der gescannten Dateien
- Anzahl der infizierten Dateien
- vollständiger Pfad der infizierten Dateien
- Scan-Dauer
- während des Scans durchgeführte Aktionen oder aufgetretene Fehler

Quarantäne

Die Hauptaufgabe der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Endpoint Security fälschlicherweise erkannt worden sind.

Die Dateien in der Quarantäne können in einem Log angezeigt werden, das Datum und Uhrzeit der Quarantäne und den ursprünglichen Speicherort der infizierten Dateien enthält.

Um eine Datei aus der Quarantäne an ihrem ursprünglichen Speicherort wiederherzustellen, tippen Sie darauf und wählen **Wiederherstellen**. Diese Option wird nicht empfohlen.

Um eine Datei aus der Quarantäne endgültig von Ihrem Gerät zu löschen, tippen Sie darauf und wählen **Löschen**. Wenn Sie alle Dateien aus der Quarantäne entfernen möchten, drücken Sie die **Menü**-Taste und tippen auf **Alles löschen**.

Einstellungen

Mit den Einstellungen im Bereich **On-Demand** können Sie die Parameter für manuelle gestartete Scans (On-Demand-Scans) einrichten.

Die Option **Warnung anzeigen** bewirkt, dass jedes Mal eine Warnung angezeigt wird, wenn eine neue Bedrohung vom On-Demand-Scanner erkannt wird.

Wenn Sie alle auf Ihrem Gerät installierten Apps (*.apk*-Dateien) scannen möchten, wählen Sie **Apps scannen**.

Bei der Option **Proaktiver Schutz** handelt es sich um eine algorithmusbasierte Erkennungsmethode, mit der Code analysiert und auf virentypisches Verhalten geprüft wird. Der Vorteil besteht darin, dass sich so auch Schadsoftware erkennen lässt, die noch nicht in der Signaturdatenbank enthalten ist. Allerdings erhöht sich die Scan-Dauer, wenn der proaktive Schutz aktiviert wird.

Mit der Option **Scantiefe Archive** können Sie festlegen, bis zu welcher Tiefe verschachtelte Archive (*.zip*-Dateien) gescannt werden sollen. Je höher der Wert, desto tiefer reicht die Prüfung.

Über die Option **Gespeicherte Logs** können Sie festlegen, wie viele Logs im Bereich **Scan-Logs** 5 maximal gespeichert werden.

Sie können eine **Standardaktion** festlegen, die automatisch ausgeführt wird, wenn infizierte Dateien gefunden werden. Folgende Aktionen können als Standard festgelegt werden:

- **Ignorieren** - Es wird keine Aktion mit der infizierten Datei durchgeführt (nicht empfohlen).
- **Löschen** - Die infizierte Datei wird gelöscht.
- **Quarantäne** - (Standardeinstellung) Die infizierte Datei wird in die **Quarantäne** 5 verschoben.

Unter der Einstellung **Dateitypen** werden die Dateitypen angezeigt, die auf der Android-Plattform am anfälligsten für Angriffe durch Schadsoftware sind. Aktivieren Sie die Dateitypen, die gescannt werden sollen, oder wählen Sie die Erweiterungen ab, die vom Scannen auszuschließen sind. Diese Einstellungen beziehen sich sowohl auf On-Demand-Scans als auch auf den Echtzeit-Schutz.

- **Nur gewählte Dateitypen** – Wenn Sie diese Option aktivieren, werden nur die ausgewählten Dateitypen gescannt, was zu schnelleren Scans führt. Wir empfehlen, diese Funktion gelegentlich zu deaktivieren, damit ESET Endpoint Security die Möglichkeit hat, alle möglichen Bedrohungen einschließlich solcher zu erkennen, die durch falsche Dateierweiterungen verborgen wurden.
- **DEX (Anwendungscode-Datei)** - Ausführbares Dateiformat mit kompiliertem Code für das Android-Betriebssystem.
- **SO (Bibliotheken)** - Gemeinsam genutzte Bibliotheken, die an bestimmten Orten im Dateisystem gespeichert und von verknüpften Programmen verwendet werden, die die Funktionen dieser Bibliotheken benötigen.
- **Archive (komprimierte Dateien)** - Mit dem Zip-Algorithmus komprimierte Dateien.
- **Weitere** - Sonstige bekannte Dateitypen.

Mit den Einstellungen im Bereich **Echtzeit** können Sie die Scan-Parameter für den Echtzeit-Schutz einrichten. Der Echtzeit-Schutz prüft Dateien bei jedem Zugriff in Echtzeit. Er scannt automatisch den Ordner *Download* auf der SD-Karte, Dateien aus *.apk*-Installationsdateien sowie Dateien auf der SD-Karte, nachdem diese angeschlossen wurde (sofern die Option **SD-Karte scannen** aktiviert ist). Der Echtzeit-Schutz wird beim Systemstart automatisch gestartet.

- **Echtzeit-Schutz** - Wenn diese Option aktiviert ist (Standardeinstellung), wird der Echtzeit-Schutz im Hintergrund ausgeführt.
- **Warnung anzeigen** - Diese Option bewirkt, dass jedes Mal eine Warnung angezeigt wird, wenn eine neue Bedrohung vom Echtzeit-Schutz erkannt wird.
- **SD-Karte scannen** - Bewirkt, dass Dateien vor dem Öffnen oder Speichern auf der SD-Karte gescannt werden.
- **Proaktiver Schutz** - Aktivieren Sie diese Option, um die Heuristik zu aktivieren. Die Heuristik erkennt proaktiv neue Malware, die noch nicht in der Signaturdatenbank enthalten sind, indem sie den Code analysiert und auf virentypisches Verhalten prüft. Allerdings erhöht sich die Scan-Dauer, wenn der proaktive Schutz aktiviert wird.
- **Scantiefe Archive** - Mit dieser Option können Sie festlegen, bis zu welcher Tiefe verschachtelte Archive (*.zip*-Dateien) gescannt werden sollen. Je höher der Wert, desto tiefer reicht die Prüfung.
- **Standardaktion** - Sie können eine Standardaktion festlegen, die automatisch ausgeführt wird, wenn infizierte Dateien gefunden werden. Bei der Option **Ignorieren** wird keine Aktion mit der infizierten Datei durchgeführt (nicht empfohlen). Mit **Löschen** wird die infizierte Datei gelöscht. Mit der Option **Quarantäne** wird die infizierte Datei in die **Quarantäne** 5 verschoben.

Das Meldungssymbol von ESET Endpoint Security wird links oben auf dem Bildschirm angezeigt (Android-Statusleiste). Wenn das Symbol nicht angezeigt werden soll, berühren Sie im Hauptmenü von ESET Endpoint Security die Taste **Menü**, tippen Sie auf **Meldungseinstellungen** und deaktivieren Sie **Icon anzeigen**. Bitte beachten Sie: Das rote Warnsymbol mit Ausrufezeichen, das bei Sicherheitsrisiken erscheint (z. B. Echtzeit-Schutz deaktiviert, SIM-Abgleich deaktiviert usw.), wird hierdurch nicht deaktiviert.

4. USSD-Steuerung

Die neueste Version von ESET Endpoint Security (1.2.103 und höher) schützt Ihr Android-Gerät vor Fernlöschungen und anderen USSD-Angriffen. USSD (Unstructured Supplementary Service Data)-Codes können von schädlichen Textnachrichten, QR-Codes oder URL-Links ausgeführt werden.

Wenn Sie eine Benachrichtigung zur Verfügbarkeit einer neuen Version von ESET Endpoint Security erhalten, sollten Sie die neue Version möglichst umgehend installieren.

Auf die USSD-Steuerung kann nicht über das Hauptmenü zugegriffen werden. Sie wird im Hintergrund ausgeführt und benachrichtigt Sie, wenn ein USSD-Befehl ausgeführt wird. Um Ihr Gerät ohne Sicherheitsrisiko auf USSD-Schwachstellen zu überprüfen, befolgen Sie die Anweisungen der Schritte 4–6 in diesem Knowledgebase-Artikel.

5. Antispam

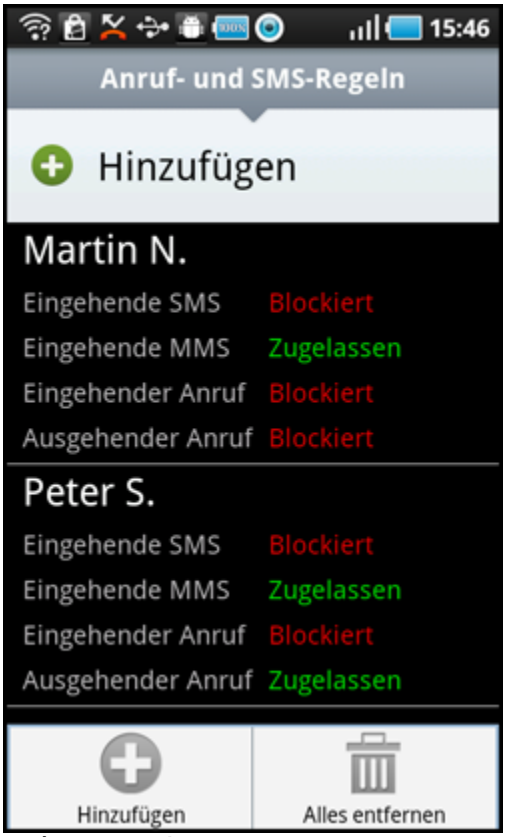
Das **Antispam**-Modul blockiert auf Grundlage der von Ihnen definierten Regeln eingehende SMS/MMS sowie ein- und ausgehende Anrufe.

Solche unerwünschten Nachrichten sind zum Beispiel Werbung von Mobilfunkanbietern oder Nachrichten von unbekannten Benutzern. Der Ausdruck *Kontakte blockieren* bezieht sich auf das automatische Verschieben von eingehenden Nachrichten in den Bereich **Spam-Logs** 7. Es wird kein Hinweis angezeigt, wenn eine eingehende Nachricht blockiert wird. Der Vorteil dieses Verfahrens besteht darin, dass Sie einerseits nicht durch unerwünschte Informationen belästigt werden, andererseits jedoch auch die Logs nach Nachrichten durchsuchen können, die fälschlicherweise blockiert worden sind.

Zum Hinzufügen einer neuen Antispam-Regel tippen Sie auf **Anruf- und SMS-Regeln** > **Hinzufügen**. Geben Sie die zu blockierende Telefonnummer ein oder tippen Sie auf **+**, um sie aus Ihrer Kontaktliste auszuwählen. Geben Sie an, ob durch diese Regel Nachrichten und Anrufe blockiert oder zugelassen werden sollen, und tippen Sie abschließend auf **Fertig**.

Um eine vorhandene Regel zu bearbeiten oder zu entfernen, halten Sie den betreffenden Eintrag gedrückt und wählen die gewünschte Aktion. Wenn Sie alle Antispam-Regeln entfernen möchten, drücken Sie die **Menü**-Taste und tippen auf **Alles entfernen**.

HINWEIS: Die Telefonnummer muss mit der internationalen Vorwahl beginnen, gefolgt von der eigentlichen Telefonnummer (z. B. +16101001000).



Antispam-Regeln

Einstellungen

Anonyme Anrufer blockieren - Aktivieren Sie diese Option, um Anrufer zu blockieren, die die Übermittlung ihrer Telefonnummer absichtlich über die CLIR-Funktion (Calling Line Identification Restriction) ausgeschaltet haben.

Bekannte Kontakte blocken - Aktivieren Sie diese Option, um Nachrichten und Anrufe für Kontakte zu blockieren, die in Ihrer Kontaktliste enthalten sind.

Unbekannte Kontakte blocken - Aktivieren Sie diese Option, um Nachrichten und Anrufe für Kontakte zu blockieren, die nicht in Ihrer Kontaktliste enthalten sind. Diese Option können Sie verwenden, um unerwünschte Telefonanrufe (z. B. von Telemarketing-Firmen) zu unterbinden oder um zu verhindern, dass Kinder unbekannte Nummern wählen. (Hierzu empfiehlt es sich außerdem, Ihre Antispam-Einstellungen mit einem **Passwort** 11 zu schützen.)

Im Bereich **Spam-Logs** können Sie die Anrufe und Nachrichten anzeigen, die vom Antispam-Modul blockiert wurden. Jeder Log-Eintrag enthält Name, Datum und Uhrzeit des Ereignisses sowie die dazugehörige Telefonnummer. Bei blockierten SMS ist auch die eigentliche Nachricht enthalten.

6. Anti-Theft

Die **Anti-Theft**-Funktion schützt Ihr Mobiltelefon vor unerlaubtem Zugriff.

Bei Verlust oder Diebstahl Ihres Mobiltelefons wird Ihr Mobiltelefon automatisch von ESET Endpoint Security gesperrt, sobald Ihre SIM-Karte durch eine neue (nicht vertrauenswürdige) ersetzt wird. Außerdem wird eine Alarm-SMS an benutzerdefinierte Telefonnummern gesendet. Diese Nachricht enthält die Telefonnummer der aktuell verwendeten SIM-Karte, die IMSI-Nummer (International Mobile Subscriber Identity) und die IMEI-Nummer des Telefons (International Mobile Equipment Identity). Dem nicht autorisierten Benutzer ist nicht bewusst, dass diese Nachricht gesendet wurde, da sie automatisch aus dem Ordner **SMS/MMS** gelöscht wird. Außerdem können Sie ein verloren gegangenes Mobiltelefon über seine GPS-Koordinaten orten lassen oder alle darauf gespeicherten Daten aus der Ferne löschen.

Vertrauenswürdige SIM

Diese Funktionalität betrifft nur Geräte mit SIM-Karte (keine Tablets oder CDMA-Telefone).

Wenn Sie die aktuell in Ihrem Mobiltelefon eingesetzte SIM-Karte als „vertrauenswürdig" speichern möchten, tippen Sie auf die Schaltfläche **Hinzufügen**. Bei Verwendung mehrerer SIM-Karten ist es sinnvoll, diese durch Änderung der Angabe **Alias der SIM** zu kennzeichnen (z. B. *Büro*, *Zuhause* usw.).

Um einen vorhandenen SIM-Eintrag zu bearbeiten oder zu entfernen, halten Sie den betreffenden Eintrag gedrückt und wählen Sie **Bearbeiten** bzw. **Entfernen**. Wenn Sie alle Einträge aus der Liste entfernen möchten, drücken Sie die **Menü**-Taste und tippen auf **Alles entfernen**.

Administratorkontakte

In der Liste **Administratorkontakte** können Sie mit der Option **Hinzufügen** die Telefonnummern definieren, die eine Alarm-SMS erhalten sollen, wenn eine nicht vertrauenswürdige SIM-Karte in Ihr Gerät eingesetzt wurde. Geben Sie unter **Name des Kontakts** den Namen der Person und unter **Telefonnummer** ihre Telefonnummer ein, oder wählen Sie den Kontakt mit der Schaltfläche **+** aus Ihrer Kontaktliste aus. Wenn der Kontakt mehrere Telefonnummern enthält, wird die Alarm-SMS an sämtliche Telefonnummern gesendet.

Um einen vorhandenen Eintrag zu bearbeiten oder zu entfernen, halten Sie den betreffenden Eintrag gedrückt und wählen Sie **Bearbeiten** oder **Entfernen** aus. Wenn Sie alle Einträge aus der Liste entfernen möchten, drücken Sie die **Menü**-Taste und tippen auf **Alles entfernen**.

HINWEIS: Die Telefonnummer muss mit der internationalen Vorwahl beginnen, gefolgt von der eigentlichen Telefonnummer (z. B. +16101001OO).

Einstellungen

Wenn Sie den SIM-Abgleich nicht ausführen möchten, wählen Sie die Option **SIM-Abgleich deaktivieren**. Hiermit werden die roten *Sicherheitsrisiko!*-Warnungen (*SIM-Abgleich ist deaktiviert* und *Keine vertrauenswürdige SIM definiert*) im Hauptmenü von ESET Endpoint Security deaktiviert. Auf CDMA-Geräten ist die Option „SIM-Abgleich deaktivieren" nicht verfügbar.

Um die automatische Prüfung der verwendeten SIM-Karte (und damit eine mögliche Sendung von Alarm-SMS) einzuschalten, aktivieren Sie die Option **SIM-Abgleich aktivieren**.

Im Feld **Alarm-SMS Text** können Sie den Text festlegen, der an die vorab festgelegte(n) Nummer(n) gesendet wird, nachdem eine nicht vertrauenswürdige SIM in Ihr Gerät eingesetzt wurde. Sie können auch eine andere E-Mail-Adresse oder Nummer eingeben.

SMS-Kommandos

SMS-Remotekommandos (Löschen, Sperren, Orten) funktionieren nur, wenn **SMS-Kommandos erlauben** aktiviert ist.

Mit der Option **SMS-Passwd-Reset erlauben** können Sie Ihr Sicherheitspasswort zurücksetzen, indem Sie eine SMS von einer unter **Administratorkontakte** gespeicherten Nummer an Ihre Mobilfunknummer schicken. Diese SMS muss das folgende Format haben: *eset remote reset*

Wenn Sie Ihr Telefon verloren haben und es sperren möchten, senden Sie von einem beliebigen Mobilgerät eine SMS im folgenden Format an Ihre Telefonnummer:
eset lock Passwort
Ersetzen Sie dabei *Passwort* durch Ihr eigenes Passwort, das Sie im Bereich **Passwort** festgelegt haben. Unbefugte Benutzer können dann nichts mit Ihrem Telefon anfangen, da zur Nutzung zunächst Ihr Passwort eingeben werden muss.

Um die GPS-Koordinaten Ihres Mobilgeräts abzufragen, senden Sie eine SMS mit dem folgenden Format an Ihre Mobilfunknummer bzw. die Nummer der aktuell eingelegten SIM-Karte:
eset find Passwort
Sie erhalten dann eine SMS mit GPS-Koordinaten und einem Link zu einer Google Maps-Karte, aus der der genaue Standort Ihres Mobilgeräts ersichtlich ist. Beachten Sie, dass die GPS-Koordinaten nur gesendet werden können, wenn das GPS-Modul Ihres Telefons zuvor bereits aktiviert wurde.

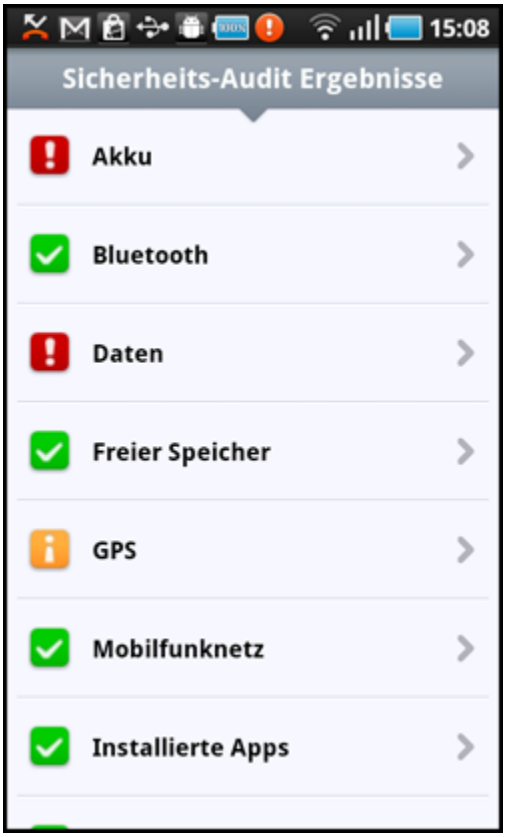
Um alle auf dem Gerät und ggf. eingelegten Wechselmedien gespeicherten Daten zu löschen, senden Sie eine SMS im folgenden Format:
eset wipe Passwort
Alle Kontakte, Nachrichten, E-Mails und installierten Apps, Ihr Google-Konto sowie der Inhalt der SD-Karte werden dann endgültig vom Gerät gelöscht. Wenn ESET Endpoint Security nicht als Geräteadministrator eingerichtet ist, werden nur Kontakte, Nachrichten und der Inhalt der SD-Karte gelöscht.

HINWEIS: Beim Passwort muss die Groß- und Kleinschreibung berücksichtigt werden. Geben Sie das Passwort also genau so ein, wie Sie es im Bereich „Passwort“ definiert haben.

7. Sicherheits-Audit

Ein **Sicherheits-Audit** prüft den Gerätestatus hinsichtlich Akku-Ladestand, Bluetooth-Status, freiem Speicherplatz usw.

Um ein Sicherheits-Audit manuell zu starten, tippen Sie auf **Audit**. Daraufhin wird ein detaillierter Bericht angezeigt.



Sicherheits-Audit: Ergebnisse

Ein grünes Häkchen bedeutet, dass der Wert über dem Grenzwert liegt oder dass der entsprechende Punkt kein Sicherheitsrisiko darstellt.

Ein gelbes Symbol bedeutet, dass mindestens ein Wert unter dem Grenzwert liegt oder dass der entsprechende Punkt ein potenzielles Sicherheitsrisiko darstellt. Für weitere Informationen tippen Sie auf den betreffenden Punkt.

Ein rotes Ausrufezeichen bedeutet, dass der Wert unter dem Grenzwert liegt oder dass der entsprechende Punkt ein Sicherheitsrisiko darstellt und daher korrigiert werden sollte.

Wenn Sie ein rot hervorgehobenes Problem beheben lassen möchten, tippen Sie auf den betreffenden Punkt und bestätigen die Abfrage mit **Ja**.

Einstellungen

Das Sicherheits-Audit wird standardmäßig alle 24 Stunden ausgeführt. Wenn Sie die regelmäßigen Audits abschalten möchten, deaktivieren Sie die Optionen **Regelmäßiges Audit**.

Ist die Option **Automatisch beheben** aktiviert, versucht ESET Endpoint Security automatisch, die riskanten Elemente (z. B. Bluetooth-Status) ohne Benutzereingriff zu beheben. Diese Option betrifft nur regelmäßige (geplante) Audits.

Über die Option **Gespeicherte Logs** können Sie festlegen, wie viele Logs im Bereich **Audit-Logs** maximal gespeichert werden.

Über die Option **Auditintervall** können Sie einstellen, wie häufig ein regelmäßiges (geplantes) Audit durchgeführt werden soll.

Und den Grenzwert einzustellen, ab dem der freie Speicher und der Akku-Ladestand als „niedrig" interpretiert werden, verwenden Sie die Optionen **Grenzwert "Freier Speicher"** und **Grenzwert "Akku"**.

Wählen Sie auf der Registerkarte **Auditumfang** die Punkte aus, die während des regelmäßigen (geplanten) Sicherheits-Audits geprüft werden sollen.

Der Bereich **Audit-Logs** enthält Logs mit umfassenden Daten zu abgeschlossenen regelmäßigen oder manuellen Audits. Jeder Log-Eintrag enthält Datum und Uhrzeit des Ereignisses sowie ausführliche Ergebnisse zu jedem geprüften Punkt.

Der **Task-Manager** gibt Ihnen einen Überblick über alle Prozesse, Dienste und Tasks, die auf Ihrem Gerät ausgeführt werden. Mit ESET Endpoint Security können Sie Prozesse, Dienste und Tasks beenden, die nicht vom System gestartet wurden. Diese sind mit einem roten Symbol gekennzeichnet (**x**).

8. Remoteverwaltung

Mit ESET Remote Administrator (ERA) können Sie ESET Endpoint Security in einer Netzwerkumgebung direkt von einem zentralen Standort aus verwalten.

Administratoren können die folgenden Aufgaben aus der Ferne erledigen:

- Einen Konfigurations-Task in ERA erstellen und die Einstellungen an ESET Endpoint Security verteilen,
- einen On-Demand-Scan auslösen,
- Updates der Signaturdatenbank installieren,
- Log-Dateien prüfen,
- Admin-Nachrichten an Mobilgeräte senden.

ERA erhöht nicht nur Ihr Sicherheitsniveau, sondern ermöglicht auch eine komfortable Verwaltung aller ESET-Produkte, die auf Workstations und Mobilgeräten installiert sind. Von einem Mobilgerät mit ESET Endpoint Security können Sie über eine beliebige Internetverbindung (LAN, WLAN, Mobilnetz (3G, HSDPA, GPRS)) eine Verbindung zu ERA aufbauen. Es muss sich dabei lediglich um eine normale Internetverbindung ohne Proxy, Firewall usw. handeln und beide Endpunkte müssen richtig konfiguriert sein. Wenn Sie die Verbindung zu ERA über ein Mobilnetz aufbauen, hängt der Erfolg des Verbindungsversuchs vom GSM-Anbieter ab. Eine Internetverbindung mit vollem Funktionsumfang ist erforderlich. Wenn beispielsweise das Anzeigen von HTTP-Webseiten nur über Port 80 zugelassen ist, tritt beim Verbindungsversuch ein Fehler auf, weil für die Kommunikation mit dem ERA-Server der Port 2222 verwendet werden muss.

Einstellungen

Auf die Einstellungsoptionen der Remoteverwaltung können Sie über das Hauptmenü von ESET Endpoint Security zugreifen. Tippen Sie auf **Remoteverwaltung** > **Einstellungen**.

Aktivieren Sie die Remoteverwaltung mit der Option **Mit Remoteverwaltungsserver verbinden**.

Zeitabstand zwischen Verbindungen zum Server – Mit dieser Option wird festgelegt, wie oft ESET Endpoint Security eine Verbindung mit dem ERA Server aufbaut, um die Daten zu übertragen.

Primärer Server, **Sekundärer Server** – In der Regel muss nur der primäre Server konfiguriert werden. Wenn Sie mehrere ERA-Server im Netzwerk betreiben, können Sie eine Verbindung zu einem sekundären ERA Server einrichten. Diese dient als Ersatzverbindung. Falls der primäre Server nicht erreichbar ist, verbindet sich ESET Endpoint Security automatisch mit dem sekundären ERA Server. Gleichzeitig wird versucht, die Verbindung zum primären Server wiederherzustellen. Sobald diese Verbindung wieder verfügbar ist, verwendet ESET Endpoint Security wieder den primären Server. Die Einrichtung von zwei Serverprofilen für die Remoteverwaltung ist besonders für Clients geeignet, die Verbindungen aus dem lokalen Netzwerk und von außerhalb herstellen.

Serveradresse – Geben Sie entweder den DNS-Namen oder die IP-Adresse des Servers an, auf dem ERA Server läuft.

Port – Dieses Feld enthält den vorkonfigurierten Port der Verbindung. Wir empfehlen, die Standardeinstellung 2222 zu übernehmen.

Falls ESET Remote Administrator die Authentifizierung mit einem Passwort erfordert, aktivieren Sie die Option **Remoteverwaltungsserver erfordert Authentifizierung**, und geben Sie das Passwort im Feld **Passwort** ein.

HINWEIS: Weitere Hinweise zur Verwaltung Ihres Netzwerks mit ESET Remote Administrator finden Sie im ESET Remote Administrator Installation Manual and User Guide (das Dokument ist möglicherweise nicht in Ihrer Sprache verfügbar).

9. Update

Sie können ESET Endpoint Security ganz einfach auf die neueste Produktversion aufrüsten, um sicherzustellen, dass Ihr Mobilgerät vor den neuesten Bedrohungen und Angriffen geschützt ist. Wenn Sie eine Benachrichtigung zur Verfügbarkeit einer neuen Version von ESET Endpoint Security erhalten, sollten Sie die neue Version möglichst umgehend installieren.

Bei der Installation von ESET Endpoint Security sind automatische Updates standardmäßig aktiviert, damit das Programm regelmäßig aktualisiert wird. Um manuell ein Update zu starten, tippen Sie auf **Jetzt aktualisieren**.

Einstellungen

Mit der Option **Auto-Update** können Sie festlegen, in welchen Zeitabständen Signaturdatenbank-Updates automatisch heruntergeladen werden.

HINWEIS: Updates werden nur bei Bedarf ausgegeben, also wenn eine neue Bedrohung hinzugefügt wurde. So wird vermieden, dass unnötig Bandbreite in Anspruch genommen wird. Die Updates sind im Rahmen Ihrer aktiven Lizenz kostenlos. Für die Datenübertragung können jedoch bei Ihrem Mobilfunkanbieter Gebühren anfallen.

10. Passwort

Ihr Sicherheitspasswort schützt Ihre Einstellungen vor unbefugten Änderungen. Ihr Passwort benötigen Sie zum:

- Zugriff auf passwortgeschützte Funktionen von ESET Endpoint Security (Antivirus, Antispam, Anti-Theft und Sicherheits-Audit)
- Zugriff auf Ihr Telefon, nachdem dieses gesperrt wurde
- Senden von SMS-Kommandos an Ihr Gerät
- Deinstallieren von ESET Endpoint Security

HINWEIS: Der Deinstallationsschutz ist erst ab Android 2.2 verfügbar.

Um ein neues Sicherheitspasswort festzulegen, geben Sie dieses in den Feldern **Passwort** und **Passwort wiederholen** ein. Falls Sie Ihr Passwort einmal vergessen sollten, zeigt Ihnen die Option **Erinnerung** einen Hinweis an, sofern einer hinterlegt wurde.

WICHTIGER HINWEIS: Bitte wählen Sie Ihr Passwort sorgfältig aus, da es zum Entsperren Ihres Geräts sowie für die Deinstallation von ESET Endpoint Security benötigt wird.

Auf der Registerkarte **Übernehmen für** können Sie festlegen, welche Module mit dem Passwort geschützt

werden sollen.

Falls Sie Ihr Passwort einmal vergessen, können Sie eine SMS von einer Nummer aus Ihrer Liste **Administratorkontakte** an Ihre Mobilfunknummer schicken. Diese SMS muss das folgende Format haben:
eset remote reset
Ihr Passwort wird dann zurückgesetzt.

11. Fehlerbehebung und Support

11.1 Fehlerbehebung

ESET Endpoint Security bietet umfangreiche Logging-Funktionen, die bei der Diagnose technischer Probleme helfen. Wir empfehlen Ihnen, in der ESET-Knowledgebase nach einer Lösung zu suchen, bevor Sie sich an den ESET-Support wenden. Falls sich das Problem auf diesem Wege nicht lösen lässt, gehen Sie beim Kontakt mit dem ESET-Support wie folgt vor:

1. Berühren Sie im Hauptmenü von ESET Endpoint Security die Taste **Menü** und tippen Sie auf **Logging-Einstellungen**.
2. Wählen Sie die Programmkomponente, auf die sich das Problem bezieht.
3. Reproduzieren Sie das Problem. Dabei werden nun Diagnoseinformationen in eine Log-Datei geschrieben.
4. Berühren Sie im Hauptmenü von ESET Endpoint Security die Taste **Menü** und tippen Sie auf **Support**.
5. Falls Sie in unserer Knowledgebase keine Lösung gefunden haben, tippen Sie auf **Fortfahren**.
6. Füllen Sie alle Felder aus und tippen Sie unten auf dem Bildschirm auf **Senden**. Achten Sie darauf, dass dabei die Option **App-Log** aktiviert ist (standardmäßig ist dies der Fall).

11.2 Support

Bei allgemeinen oder technischen Fragen zu ESET Endpoint Security oder einem anderen Produkt von ESET stehen Ihnen unsere Support-Mitarbeiter gerne zur Verfügung.

Antworten auf die häufigsten Fragen finden Sie in der Knowledgebase von ESET unter folgendem Link:
http://kb.eset.com/android

Die ESET-Knowledgebase enthält eine Vielzahl an nützlichen Informationen zur Lösung der häufigsten Probleme. Sie ist nach Kategorien gegliedert und verfügt über eine erweiterte Suchfunktion.

Wenn Sie sich an den Support von ESET wenden möchten, verwenden Sie dazu das Anfrageformular unter folgendem Link:
http://eset.com/support/contact

Um direkt vom Mobiltelefon eine Supportanfrage zu senden, berühren Sie im Hauptmenü von ESET Endpoint Security die Taste **Menü** und tippen Sie auf **Support**. Füllen Sie alle Felder aus. Um ein vollständiges **App-Log** an Ihre Anfrage anzuhängen, gehen Sie wie im Abschnitt Fehlerbehebung 12 beschrieben vor.